

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

ALEXANDRIA RUDOLPH, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

HUDSON'S BAY COMPANY, a Canadian
corporation; SAKS FIFTH AVENUE LLC, a
Massachusetts limited liability company; SAKS &
COMPANY LLC, a Delaware limited liability
company; SAKS INCORPORATED, a Tennessee
corporation; LORD & TAYLOR LLC, a Delaware
limited liability company,

Defendants.

No. 1:18-cv-08472-PKC

**PLAINTIFF'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS'
MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT**

TABLE OF CONTENTS

I. INTRODUCTION..... 1

II. STATEMENT OF FACTS..... 2

III. ARGUMENT..... 3

 A. Plaintiff Has Alleged An Injury In Fact Under Article III..... 3

 1. The Substantial Risk That Future Identity Theft Will Occur Is
 Sufficient Harm To Confer Article III Standing..... 4

 2. Plaintiff’s Allegations Concerning Lost Money and Time Are
 Sufficient to Confer Article III Standing 6

 3. The Deprivation In Value Of Plaintiff’s Personal Information Is
 An Injury In Fact..... 10

 4. Plaintiff Also Suffered Article III Injury By Not Receiving The
 Benefit Of The Bargain..... 11

 5. Defendants Misconstrue Plaintiffs’ Allegations Regarding Fraudulent
 Charges On Her Account and Loss of Access to Account Funds..... 11

 B. Plaintiff’s Common Law Claims Are Sufficiently Alleged..... 12

 1. Plaintiff Has Adequately Pleaded Her Negligence Claim 12

 2. Plaintiff Has Adequately Alleged A Claim For Negligence *Per Se* 15

 3. Plaintiff Has Adequately Pleaded Her Implied Contract Claim 16

 4. Plaintiff Has Adequately Alleged Her Unjust Enrichment Claim 18

 C. Plaintiff’s Statutory Claims Should Also Survive 20

 1. Plaintiff Can Establish A Private Right of Action Under the
 Mississippi Consumer Protection Act..... 20

 2. Plaintiff Has Alleged a Cognizable Injury Under The California
 Customer Records Act 21

 3. Plaintiff Has Alleged a Cognizable Injury Under The UCL..... 23

 D. Plaintiff’s Declaratory and Injunctive Relief Claim Should Survive 25

IV. CONCLUSION 25

TABLE OF AUTHORITIES

Cases	Page(s)
<i>532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc.</i> , 96 N.Y.2d 280 (2001)	14
<i>In re Adobe Sys., Inc. Privacy Litig.</i> , 66 F. Supp. 3d 1197 (N.D. Cal. 2014)	<i>passim</i>
<i>Anderson v. Hannaford Bros.</i> , 659 F.3d 151 (1st Cir. 2011)	8
<i>In re Anthem, Inc. Data Breach Litig.</i> , 162 F. Supp. 3d 953 (N.D. Cal. 2016)	18, 19
<i>In re Anthem, Inc. Data Breach Litig.</i> , No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016)	6, 19, 24
<i>In re Arby's Rest. Grp. Inc. Litig.</i> , No. 1:17-CV-0514-at, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018)	25
<i>Astiana v. Hain Celestial Grp.</i> , 783 F.3d 753 (9th Cir. 2015)	19
<i>Atl. Marine Const. Co. v. U.S. Dist. Court for W. Dist. of Texas</i> , 571 U.S. 49 (2013)	12
<i>Attias v. Carefirst, Inc.</i> , 865 F.3d 620 (D.C. Cir. 2017)	4
<i>Booker v. S.C. Dep't of Corr.</i> , 855 F.3d 533 (4th Cir. 2017)	4
<i>Braddock v. Orlando Reg'l Health Care Sys., Inc.</i> , 881 F. Supp. 580 (M.D. Fla. 1995)	21
<i>Castillo v. Seagate Tech.</i> , LLC, No. 16-CV-01958-RS, 2016 WL 9280242 (N.D. Cal. Sept. 14, 2016)	16, 17, 18
<i>Caudle v. Towers, Perrin, Forster & Crosby, Inc.</i> , 580 F. Supp. 2d 273 (S.D.N.Y. 2008)	13
<i>Century Pac., Inc. v. Hilton Hotels Corp.</i> , No. 03 CIV. 8258 (SAS), 2004 WL 868211 (S.D.N.Y. Apr. 21, 2004)	14
<i>ChromaDex, Inc. v. Elysium Health, Inc.</i> , No. SACV 16-02277-CJC, 2017 WL 7080237 (C.D. Cal. Nov. 28, 2017)	18

<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	9, 10
<i>Corona v. Sony Pictures Entm’t, Inc.</i> , No. 14-CV-09600 RGK (Ex), 2015 WL 3916744 (C.D. Cal. June 15, 2015).....	15
<i>DC Comics v. Pac. Pictures Corp.</i> , No. CV 10-03633 ODW, 2011 WL 13124665 (C.D. Cal. May 25, 2011).....	5
<i>Dent v. Nat’l Football League</i> , 902 F.3d 1109 (9th Cir. 2018)	16
<i>Dieffenbach v. Barnes & Noble, Inc.</i> , 887 F.3d 826 (7th Cir. 2018)	7, 23
<i>Dugas v. Starwood Hotels & Resorts Worldwide, Inc.</i> , No. 3:16-CV-00014-GPC-BLM, 2016 WL 6523428 (S.D. Cal. Nov. 3, 2016).....	7
<i>Engl v. Nat. Grocers by Vitamin Cottage, Inc.</i> , No. 15-CV-02129-MSK-NYW, 2016 WL 8578252 (D. Colo. Sept. 21, 2016).....	10, 24
<i>In re Experian Data Breach Litig.</i> , No. SACV 15-1592, 2016 WL 7973595 (C.D. Cal. Dec. 29, 2016)	<i>passim</i>
<i>In re Facebook Privacy Litig.</i> , 572 F. App’x 494 (9th Cir. 2014)	11
<i>Fero v. Excellus Health Plan, Inc.</i> , 236 F. Supp. 3d 735 (W.D.N.Y. 2017)	3, 19
<i>First Choice Fed. Credit Union v. Wendy’s Co.</i> , No. CV 16-506, 2017 WL 9487086 (W.D. Pa. Feb. 13, 2017)	25
<i>Forth v. Walgreen Co.</i> , No. 17-CV-2246, 2018 WL 1235015 (N.D. Ill. Mar. 9, 2018).....	20
<i>Galaria v. Nationwide Mut. Ins. Co.</i> , 663 F. App’x 384 (6th Cir. 2016)	4
<i>Golden Pac. Bancorp v. F.D.I.C.</i> , 273 F.3d 509 (2d Cir. 2001).....	18
<i>Gordon v. Chipotle Mexican Grill, Inc.</i> , No. 17-CV-1415-CMA-MLC, 2018 WL 3653173 (D. Colo. Aug. 1, 2018).....	8, 10, 23
<i>Hameed-Bolden et al. v. Forever 21 Retail, Inc.</i> , No. CV18-03019 SJO, 2018 WL 6802818 (C.D. Cal. Oct. 1, 2018)	16, 17, 23

<i>In re Horizon Healthcare Servs. Inc. Data Breach Litig.</i> , 846 F.3d 625 (3d Cir. 2017).....	4
<i>Irwin v. Jimmy John’s Franchise, LLC</i> , 175 F. Supp. 3d 1064 (C.D. Ill. 2016)	17
<i>Kwikset Corp. v. Super. Crt.</i> , 51 Cal. 4th 310 (2011)	23
<i>Leibowitz v. Cornell Univ.</i> , 584 F.3d 487 (2d Cir. 2009).....	16
<i>Lewert v. P.F. Chang’s China Bistro, Inc.</i> , 819 F.3d 963 (7th Cir. 2016)	<i>passim</i>
<i>In re LinkedIn User Privacy Litig.</i> , No. 5:12-cv-3088-EJD, 2014 WL 1323713 (N.D. Cal. Mar. 28, 2014)	11
<i>Lisk v. Lumber One Wood Preserving, LLC</i> , 792 F.3d 1331 (11th Cir. 2015)	20
<i>Powell v. McCormack</i> , 395 U.S. 486 (1969).....	25
<i>Remijas v. Neiman Marcus Grp.</i> , 794 F.3d 688 (7th Cir. 2015)	9
<i>Robinson v. Corr. Med. Assocs., Inc.</i> , No. 1:09-CV-01509-JOF, 2010 WL 2499994 (N.D. Ga. June 15, 2010).....	21
<i>Sackin v. TransPerfect Glob., Inc.</i> , 278 F. Supp. 3d 739 (S.D.N.Y. 2017).....	<i>passim</i>
<i>Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.</i> , 559 U.S. 393 (2010).....	20
<i>Sheet Metal Workers Local No. 20 Welfare & Benefit Fund v. CVS Health Corp.</i> , 221 F. Supp. 3d 227 (D.R.I. 2016).....	20
<i>In re Sony Gaming Networks & Customer Data Sec. Breach Litig.</i> , 996 F. Supp. 2d 942 (S.D. Cal. 2014).....	22
<i>Suchanek v. Sturm Foods, Inc.</i> , 311 F.R.D. 239 (S.D. Ill. 2015)	20
<i>Suez Equity Investors, L.P. v. Toronto-Dominion Bank</i> , 250 F.3d 87 (2d Cir. 2001).....	15

<i>In re SuperValu, Inc., Customer Data Sec. Breach Litig.,</i> No. 14-MD-2586, 2018 WL 1189327 (D. Minn. Mar. 7, 2018)	12
<i>Svenson v. Google, Inc.,</i> No. 13-cv-4080, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015).....	10
<i>In re Target Corp. Data Sec. Breach Litig.,</i> 66 F. Supp. 3d 1154 (D. Minn. 2014).....	18, 19
<i>In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.,</i> No. 1:14-MD-2583-TWT, 2016 WL 2897520 (N.D. Ga. May 18, 2016).....	25
<i>Those Certain Interested Underwriters, at Lloyd's, London, subscribing to Policy</i> <i>No. Z101663/003 v. Farley Grp.,</i> No. 1:12-CV-0707, 2015 WL 5602924 (N.D.N.Y. Sept. 23, 2015).....	14
<i>Torres v. Wendy's Int'l, LLC,</i> No. 6:16-CV-210-ORL-40DCI, 2017 WL 8780453 (M.D. Fla. Mar. 21, 2017).....	7
<i>Walters v. Kimpton Hotel & Rest. Grp., LLC,</i> No. 16-cv-05387-VC, 2017 WL 1398660 (N.D. Cal. Apr. 13, 2017).....	<i>passim</i>
<i>Whalen v. Michaels Stores, Inc.,</i> 689 F. App'x 89 (2d Cir. 2017)	<i>passim</i>
<i>In re Yahoo! Inc. Customer Data Sec. Breach Litig.,</i> No. 16-MD-2752-LHK, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017).....	<i>passim</i>
<i>In re Zappos.com, Inc.,</i> 108 F. Supp. 3d 949 (D. Nev. 2015).....	24
<i>In re Zappos.com, Inc.,</i> 888 F.3d 1020 (9th Cir. 2018)	4, 5

Statutes

Cal. Civ. Code §1798.81.5.....	21
Cal. Civ. Code §1798.82(d)(1)	22
Cal. Civ. Code §1798.84(e)	22
Federal Rule of Civil Procedure 23	20, 21
Federal Rule of Civil Procedure 8	19, 21

Other Authorities

Federal Practice & Procedure § 1758 (3d ed. 2018).....20

Plaintiff Alexandria Rudolph (“Plaintiff”) respectfully submits the following Memorandum of Law in Opposition to Defendants Hudson’s Bay Company, Saks Fifth Avenue LLC, Saks & Company LLC, Saks Incorporated, and Lord & Taylor LLC’s (collectively, “Defendant” or “Saks”) Motion to Dismiss Plaintiff’s Second Amended Complaint (“MTD”).

I. INTRODUCTION

Defendants were aware of their inadequate data security standards leading up to the theft of over five million customer payment card accounts. Indeed, Saks’ data security failures are not an isolated event. A mere two months before hackers successfully stole and exploited this data, Saks had discovered that tens of thousands of their customers’ personal information were exposed to the public in a separate security incident. Further, one month before the data breach, Saks explicitly stated that their data security measures “may be undermined” and could lead to theft of their customers’ personal information. Despite these warning signs and warranting on their website that they would protect their customers’ private data, Saks failed to maintain adequate data security standards, leading to the massive data breach at the heart of this action.

As a shopper at Saks, Plaintiff’s customer data was stolen in the data breach, leading to Plaintiff’s bank account being frozen. As a consequence, Plaintiff had no choice but to expend considerable resources dealing with Defendants’ failures. Moreover, Plaintiff is now at significant risk of future identify theft as criminals still have her private data. Nonetheless, Defendants seek to escape liability by arguing that Plaintiff’s injuries do not suffice under the broad, lenient scope of Article III. Defendants’ arguments have been rejected by a majority of courts across the nation, which have recognized that such injuries are sufficient to confer Article III standing. Defendants’ remaining arguments, predominantly focused on harm, fail on similar grounds. For these reasons, and as further set forth below, Defendants’ MTD should be denied.

II. STATEMENT OF FACTS

This putative class action challenges Defendants’ failure to secure and safeguard their customers’ credit and debit card data. Second Amended Complaint (“SAC”), Dkt. No. 75, at ¶ 1. Specifically, starting in May 2017, hackers breached Defendants’ point-of-sale systems and began syphoning customers’ private financial information (the “Data Breach”). *Id.* at ¶¶ 3-5. Due to Defendants’ lax security, the Data Breach went undetected for nearly a year before a third-party researcher informed Defendants that they had been hacked. *Id.* at ¶ 5. By then, the private data of over 5 million customer’s cards had been stolen, with many cards having already been put up for sale to the highest bidder on the dark web. *Id.* at ¶¶ 78-79. Among the information stolen was customers’ first and last names, the expiration date of their payment cards, their primary account number, and their CVVs (three or four number security code on the card) (“Customer Data”). This Data Breach was not an isolated event, as a mere two months before the Data Breach started, Defendants inadvertently “exposed the personal information of tens of thousands of [Saks Fifth Avenue] customers through the company’s websites” to the public. *Id.* at ¶ 9. One month prior to the Data Breach, Saks had explicitly stated that their data security measures “may be undermined” and could lead to theft of their customers’ personal information.

On November 23, 2017, during the period of the Data Breach, Plaintiff shopped with her Visa debit card at a Saks store in Beverly Hills, California. *Id.* at ¶ 21. On May 18, 2018, Plaintiff’s bank notified her of fraudulent activity on her debit card used at Saks and, as a result, froze Plaintiff’s bank account. *Id.* at ¶ 22. Plaintiff suffered the following subsequent injuries: (1) Plaintiff spent numerous hours contacting her bank and communicating with its staff regarding the fraudulent activity and freeze on her account, requesting and obtaining a new debit card, and reviewing her financial account records immediately after her account was frozen; (2) Because

Plaintiff needed a new debit card immediately to purchase basic necessities, Plaintiff drove approximately 25 miles (which took her about one and a half hours) to the bank branch to get a new card. In doing so, Plaintiff expended approximately 1.20 gallons of gasoline, which cost her approximately \$4.68; (3) Since May 2018, Plaintiff has spent numerous hours reviewing her monthly financial statements for fraud and updating her payment card information with various retailers. *Id.* (see for specific hours alleged). Plaintiff would not have spent the foregoing time and money otherwise had it not been for the Data Breach. *Id.*

Plaintiff would not have shopped at Saks at all during the Data Breach had she been aware of Defendants' lax data security practices. *Id.* at ¶¶ 23, 25. Plaintiff also suffered injury in the form of diminution in the value of her Customer Data and the continuing risk of additional future identity theft as a result of her private data being stolen. *Id.* at ¶ 27. This risk is exacerbated by the fact that as of April 1, 2018, approximately 125,000 payment card records have been released for sale, with experts "expect[ing] the entire cache to become available in the [future]." *Id.* at ¶ 79.

III. ARGUMENT

A. Plaintiff Has Alleged An Injury In Fact Under Article III

Defendants contend that Plaintiff lacks standing under Article III of the U.S. Constitution because she purportedly failed to allege an "injury in fact."¹ MTD at 6. Defendants reason that certain categories of injury alleged by Plaintiff are insufficient to confer Article III standing, and advance arguments in support. *Id.* at 6-11. Plaintiff addresses each argument in turn.

¹ To be clear, Defendants do not explicitly challenge that Plaintiff has not met the "fairly traceable" and "likely to be redressed" elements of Article III standing. To the extent Defendants attempt to make a causation argument (*see* MTD at 8), the argument nonetheless fails. *See Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 758 (W.D.N.Y. 2017) (finding misuse of customer data "fairly traceable" to the data breach when plaintiffs alleged that defendants failed to safeguard their customer data, hackers gained access to the data, and defendants' failure led to identity theft).

1. The Substantial Risk That Future Identity Theft Will Occur Is Sufficient Harm To Confer Article III Standing

As an initial matter, because Defendants rely heavily on *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) throughout their MTD, Plaintiff will first address *Whalen*, and will reiterate such arguments in subsequent sections to the extent necessary.

Despite Defendants' extensive reliance on *Whalen*, *Whalen* is both non-binding and inapposite to the facts at hand. As Defendants admit, *Whalen* is a summary order and "Second Circuit rulings by summary order do not have precedential effect[.]" MTD at 7, n.3; *see Whalen*, 689 F. App'x at 89 (noting that the case is a summary order with no precedential effect); *see also* 2d Cir. Local R. 32.1.1(a) ("Rulings by summary order do not have precedential effect"). Indeed, at least one federal court, presiding over the world's largest data breaches to date, has declined to follow *Whalen* as unpersuasive unpublished authority. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-2752-LHK, 2017 WL 3727318 at *15 (N.D. Cal. Aug. 30, 2017) (noting that *Whalen* is an unpublished and non-binding summary order, even in the Second Circuit).

Unlike some of its sister Circuits, the Second Circuit has yet to issue a binding decision on Article III standing in the context of data breach actions. However, the majority of sister Circuits that have considered the issue have held that the prospect of future identity theft alone is sufficient for Article III standing. *See Attias v. Carefirst, Inc.*, 865 F.3d 620, 627-28 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 638-39 (3d Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965-67 (7th Cir. 2016); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018).²

² In the absence of controlling law in this Circuit, this Court should follow the majority view. *Booker v. S.C. Dep't of Corr.*, 855 F.3d 533, 539 n.2 (4th Cir. 2017), *cert. denied* 138 S. Ct. 755 (2018) ("Following the Supreme Court's lead, several of our sister circuits, like us, have recognized that courts may consider decisions from other circuits in

Under the majority view, an allegation of future injury suffices if there is a “substantial risk that the harm will occur.” *Zappos*, 888 F.3d at 1026 (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013)). In *Zappos*, the court found that the mere increased risk of future identity theft from hackers having the plaintiffs’ personal information (leading to a high risk of future “phishing” and “pharming” of other personal information) was a sufficient to confer Article III standing. *Id.* at 1027, 1029; *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, at 1214–15 (N.D. Cal. 2014) (holding that plaintiffs were under an “imminent” threat of harm when hackers had not misused, but may misuse, their personal information). Here, Plaintiff has similarly alleged a continuing and impending risk of additional future fraud and identity theft based on hackers’ obtaining similar private information. SAC at ¶ 27. Plaintiff’s risk of future injury is even more substantial than in *Zappos* given that she has already incurred fraudulent charges on her account, and the payment cards exposed in the breach have already been exposed and will likely continue to be exposed on the dark web.³ *Id.* at ¶¶ 27, 79.

Defendants’ contention that there is no future risk because Plaintiff’s card has already been canceled is unavailing. MTD at 7-8. As further discussed below in Section III.A.2, a criminal can use a stolen credit card to open a new card or commit other identity theft under Plaintiff’s name. *Lewert*, 819 F.3d at 967 (7th Cir. 2016) (“Kosner has already cancelled his debit card, but he is still at risk of identity theft.”). Further, Plaintiff has already been harmed regardless of any reimbursements. *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG (DFMx), 2016 WL

the absence of binding precedent.”); *DC Comics v. Pac. Pictures Corp.*, No. CV 10-03633 ODW (RZx), 2011 WL 13124665, at *2 (C.D. Cal. May 25, 2011) (following First Circuit precedent, explaining that “[i]n the absence of controlling authority from the Ninth Circuit, this Court follows the majority perspective.”)

³ Plaintiff also has standing under the majority view based on the mere fact that she incurred fraudulent charges on her account. *Zappos*, 888 F.3d at 1024 (explaining, and not overturning, the district court’s finding that the “first group of plaintiffs had Article III standing because they alleged ‘that actual fraud occurred as a direct result of the breach’”); *Adobe*, 66 F. Supp. 3d at 1215 (holding that while theft of personal information without misuse is still an injury, “the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused.”).

7973595, at *3 (C.D. Cal. Dec. 29, 2016) (finding that plaintiff was injured in spending time addressing the fraudulent activity and “detect[ing]” future identity theft, even when he was reimbursed for the fraudulent charges).

In any event, if the Court is inclined to follow *Whalen* rather than the majority view, Plaintiff’s allegations extend past *Whalen*, as Plaintiff has alleged *specific*, actual out-of-pocket costs (\$4.68) and lost time spent dealing with the Data Breach. Conversely, in *Whalen*, the plaintiff generically alleged injuries⁴ with “no specifics about any time or effort that she herself has spent monitoring her credit[,]” which is what distinguished the case from *Lewert*. *Whalen*, 689 F. App’x at 91 n.1.; *c.f.*, *Lewert* 819 F.3d at 967 (conferring Article III standing in a data breach, in part, because plaintiff alleged specific dollars expended as a consequence of the breach, as well as time spent monitoring his accounts).

2. Plaintiff’s Allegations Concerning Lost Money and Time Are Sufficient to Confer Article III Standing

As discussed above, Plaintiff expended \$4.68 and several hours remediating the fraud and monitoring her accounts to prevent further injury. Courts have routinely held that such injuries are specific, non-speculative, and concrete, and are therefore sufficient for Article III standing. *See, e.g., Yahoo!*, 2017 WL 3727318 at *15 (distinguishing *Whalen* and finding that consequential fees, and time spent monitoring accounts, are adequate injuries for Article III standing); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 746–47 (S.D.N.Y. 2017) (“[A] plaintiff’s expenses in taking reasonable measures to prevent the harm’s fruition also may be viewed as an injury in fact.”); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *16

⁴ Specifically, the plaintiff in *Whalen* alleged that: “Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Michaels’ wrongful conduct, particularly given the incidents of actual misappropriation from Class members’ financial accounts, as detailed above.” *See* Declaration of Timothy J. Peter (“Peter Decl.”), Ex. 1, *Whalen* Complaint, at ¶ 52. “Plaintiff and the Class Suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.” *Id.*, at ¶ 54.

(N.D. Cal. May 27, 2016) (“*Anthem II*”) (holding that consequential out of pocket expenses are sufficient damages); *Walters v. Kimpton Hotel & Rest. Grp., LLC*, No. 16-cv-05387-VC, 2017 WL 1398660, at *1 (N.D. Cal. Apr. 13, 2017) (finding plaintiff’s allegations regarding “the time and effort he has expended to monitor his credit are sufficient to demonstrate injury for standing purposes”). *Torres v. Wendy’s Int’l, LLC*, No. 6:16-CV-210-ORL-40DCI, 2017 WL 8780453, at *2 (M.D. Fla. Mar. 21, 2017) (“[Plaintiff] has articulated a concrete economic harm by alleging that he incurred a \$3 late fee as a result of the data breach in this case. Such an economic harm is sufficient to allege standing”).⁵ Plaintiff also spent considerable time updating her payment card information with various other retailers she shops with. SAC ¶ 22; *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 827 (7th Cir. 2018) (“Many people use credit or debit cards to pay bills automatically; every time the account number changes, these people must devote some of their time and mental energy to notifying merchants that the old numbers are invalid and new ones must be used.”)

To the extent Defendant uses *Whalen* to contend that Plaintiff’s cost and time allegations are insufficient, Plaintiff stands on her arguments above that *Whalen* is non-precedential. However, to the extent the Court is inclined to follow *Whalen*, Defendants’ arguments still fail for the reasons set forth below.

First, Defendants’ comparison of Plaintiff’s allegations of lost time and money to those in *Whalen* falls flat. MTD at 8-9. As discussed above, *Whalen*’s non-specific allegations regarding lost time and expenses pale in comparison to Plaintiff’s concrete allegations of specific hours and

⁵ See also *Adobe*, 66 F. Supp. 3d at 1216 (holding that costs incurred to mitigate future identity theft are sufficient to constitute injury in fact); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-CV-00014-GPC-BLM, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016) (holding that “loss of time and money spent to avoid losses caused by the data breach” is a “concrete, non-speculative harm.”); *Lewert*, 819 F.3d at 967 (holding that simply expending time monitoring account information in response to learning of a data breach is sufficient Article III injury).

dollars expended dealing with the breach. Defendants suggest that Plaintiff's allegations also fail under *Whalen* because she failed to plead specifically *why* she drove to the bank and *why* she could not wait for a replacement card. MTD at 9. This is incorrect – Plaintiff adequately alleged that as a result of her account being frozen, “[b]ecause Plaintiff *needed* a new debit card immediately” she drove to the bank and incurred costs and lost time doing so. SAC at ¶ 22. Indeed, Defendants’ argument was recently rejected in *Gordon*. See *Gordon v. Chipotle Mexican Grill, Inc.*, No. 17-CV-1415-CMA-MLC, 2018 WL 3653173 at *6-7 (D. Colo. Aug. 1, 2018), *report and recommendation adopted in part, rejected in part*, 2018 WL 4620342 (D. Colo. Sept. 26, 2018) (rejecting argument that plaintiff’s out of pocket expense to expedite delivery of new payment card was “self-inflicted,” when plaintiff reasonably incurred the expense to not forego cashback benefits on upcoming travel plans) (adopted by district court). In any event, *Whalen*’s holding in no way burdens a plaintiff to plead “specifics” as to *why* a remediating cost was immediately incurred rather than waiting, as Defendants suggest. See *Whalen* 689 F. App’x. 89, *generally*. Indeed, in the wake of fraudulent activity, it seems reasonable for an affected customer to act quickly to protect herself from further identity theft, regardless of whether those acts are ultimately effective. As simply put by the First Circuit, “the test for mitigation is not hindsight.” *Anderson v. Hannaford Bros.*, 659 F.3d 151, 165 (1st Cir. 2011).

Defendants also contend that Plaintiff’s lost time and money were not expended to “monitor her credit” under *Whalen*, or to mitigate or prevent future harm since her card was closed and account frozen. MTD at 9-10. Defendants’ arguments are unavailing. First, Plaintiff did spend several hours “monitoring her credit” to detect and prevent future harm such as further fraudulent charges. SAC at ¶ 22. Second, Defendants read *Whalen* too narrowly as affording recovery only if a plaintiff alleges time or expense “monitoring her credit.” The court in *Whalen* only dismissed

the plaintiff's allegations regarding lost time and money "monitoring her credit" because they were not alleged with "specificity." *Whalen* 689 F. App'x. 89. The *Whalen* court in no way touched on the *types or categories* of consequential expenses or time spent necessary to confer Article III standing.

Further, Defendants' argument that Plaintiff's conduct was not "mitigative" in light of her payment card being closed rings hollow because there still remains a significant risk of future *identity theft*. Defendants essentially conflate the future risk of fraudulent payment card charges with the future risk of identity theft. The latter risk lingers as criminals can use the data from a stolen payment card to open other payment cards and engage in other identity theft. *See Lewert*, 819 F.3d at 967 (distinguishing risk of fraudulent charges with the risk of identity theft, holding that even if plaintiff "has already cancelled his debit card, [] he is still at risk of *identity theft*") (emphasis added); *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015) (noting that "thieves might—and often do—acquire new credit cards unbeknownst to the victim"). Indeed, Defendants implicitly acknowledged the risk of identity theft. In their April 27, 2018 Notice of Data Breach, Defendants encourage their customers to monitor their credit, register for identity protection services, and order a credit report, rather than simply review their statements for existing affected cards. SAC at ¶ 7; *see Lewert*, 819 F.3d at 967 (finding that time spent monitoring credit reports was reasonable, particularly when defendant "encouraged consumers to monitor" the reports). Regardless, whether a data breach poses a substantial risk of future identity theft and what a plaintiff should have expected in behaving a certain way "goes to the merits." *Id.*

Contrary to Defendants' suggestion, Plaintiff in no way was "inflicting harm" upon herself, and instead was acting like an ordinary customer who reasonably incurs costs to avoid future identity theft. MTD at 9 (citing *Clapper*). In *Clapper* the Supreme Court observed that "we have

found standing based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to ***reasonably incur*** costs to mitigate or avoid that harm.” *Clapper*, 568 U.S. at 414 n.5; *Gordon*, 2018 WL 3653173 at *7 (rejecting argument that Plaintiff “self-inflicted” expense to expedite payment card to not forego cashback benefits for travel) (adopted by the district court).

Defendants rely heavily on *Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, No. 15-CV-02129-MSK-NYW, 2016 WL 8578252 (D. Colo. Sept. 21, 2016). However, the court in *Engl* noted a key deficiency, making *Engl* factually dissimilar to this case. *Id.* at *1 (noting that plaintiff had not alleged that he spent ***any*** time or effort dealing with the bank to address or resolve the fraudulent charges). Accordingly, the court held that “[w]ithout the ability to point to time and effort incurred in dealing with Visa to address the fraudulent charges actually made on his account . . . ” plaintiff did not allege actual harm. *Id.* at *7; *see also Gordon*, 2018 WL 3653173 at *5 (recognizing the same about *Engl*). Here, Plaintiff has alleged that she spent 20 minutes on the phone with the bank, 90 minutes driving to the bank, and 30 minutes at the bank, all to address and resolve the fraud. Contrary to Defendants’ position, Plaintiff was more than “inconvenienced.”

3. The Deprivation In Value Of Plaintiff’s Personal Information Is An Injury In Fact

A growing number of courts have recognized that the diminution in value of a plaintiff’s private information is also an Article III injury. *See Yahoo!*, 2017 WL 3727318, at *13 (holding that loss in value of names, email addresses, telephone numbers, birth dates, passwords, and security questions stolen in a data breach is sufficient harm for Article III standing); *Svenson v. Google, Inc.*, No. 13-cv-4080, 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015) (concluding that “[plaintiff’s] allegations of diminution in value of her personal information are sufficient to show

contract damages for pleading purposes.”).⁶ With over 125,000 payment card accounts sold as of April 1, 2018, in addition to Plaintiff’s payment card already being subject to fraudulent charges, the market for this information is clearly alive and thriving.

4. Plaintiff Also Suffered Article III Injury By Not Receiving The Benefit Of The Bargain

Plaintiff also alleges that she suffered actual injury in the form of paying money to Defendants that she would not have paid had Defendants disclosed that they lacked adequate data security practices. *See* SAC at ¶¶ 23, 25. Because Defendants never contest that this injury is inadequately pleaded or a viable Article III injury, they have waived such an argument. In any event, courts have found that “benefit of the bargain” damages are sufficient Article III injury. *See, e.g., Yahoo!*, 2017 WL 3727318 at *16-17 (finding “benefit of the bargain” losses sufficient Article III injury when defendant warranted that its services were “secure” and plaintiff paid defendant money he otherwise would not have spent had he known the services were not secure); *In re LinkedIn User Privacy Litig.*, No. 5:12-cv-3088-EJD, 2014 WL 1323713, at *9 (N.D. Cal. Mar. 28, 2014) (same).

5. Defendants Misconstrue Plaintiffs’ Allegations Regarding Fraudulent Charges On Her Account and Loss of Access to Account Funds

Defendants aver that no actual harm exists because Plaintiff fails to allege that she paid for the fraudulent charges, or that she suffered harm from being deprived of access to her account. MTD at 7-8, 10. Defendants misconstrue the thrust of Plaintiff’s allegations. Plaintiff does not allege that she was forced to pay for the fraudulent charges, nor does she allege that the deprivation of access to her funds was in and of itself an Article III harm. Rather, Plaintiff asserts that *as a result* of the fraudulent charges and lack of access to her account, she suffered and continues to

⁶ *See also In re Facebook Privacy Litig.*, 572 F. App’x 494 (9th Cir. 2014) (holding that plaintiffs adequately alleged “that they were harmed both by the dissemination of their personal information and by losing the sales value of that information” as a result of a data breach); *Experian*, 2016 WL 7973595, at *5 (recognizing that “a growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory.”).

suffer concrete and impending harm, including lost time and money, and the continued risk of additional future harm. *See* SAC ¶ 22; *see also* *Lewert*, 819 F.3d at 967 (“Even if those fraudulent charges did not result in injury to his wallet (he stated that his bank stopped the charges before they went through), he has spent time and effort resolving them.”).

B. Plaintiff’s Common Law Claims Are Sufficiently Alleged⁷

1. Plaintiff Has Adequately Pleaded Her Negligence Claim

Defendants only challenge Plaintiff’s negligence claim on damages, arguing that California and New York law require an allegation of “actual injury” to state a claim. MTD 12-13.⁸ Although Defendants concede that Plaintiff “alleged [an] ‘out-of-pocket’ loss” in gasoline expenses to obtain a replacement card, Defendants nonetheless contend that this expense was not incurred in the face of any “imminent” harm, and therefore cannot classify as an injury sufficient to state a claim for negligence. *Id.* (citing SAC ¶ 22). Defendants also omit that Plaintiff suffered an additional out-of-pocket expense in the form of time spent mitigating the harm of the data breach. SAC ¶ 22.

⁷ Because this action was transferred from California to this District by § 1404(a) transfer, this Court should apply California law to Plaintiff’s common law claims. *Atl. Marine Const. Co. v. U.S. Dist. Court for W. Dist. of Texas*, 571 U.S. 49, 65 (2013) (upon § 1404(a) transfer, a district court should apply the choice of law rules of the transferor state to determine which state’s substantive laws should apply). Here, under California’s governmental interest test, California courts would apply California law because Plaintiff is domiciled in California and completed her transaction at Saks (which ultimately led to her data being hacked) in California. *See In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *10 (D. Minn. Mar. 7, 2018) (applying law of state where plaintiff is domiciled and where he completed the transaction alleged in his claims in a data breach litigation). However, for the sake of thoroughness, Plaintiff will support her claims with authority from both jurisdictions.

⁸ Relying on a case interpreting Illinois law, Defendants later proffer a different position: that “a plaintiff must demonstrate that she suffered an out-of-pocket loss,” to establish an injury under a negligence theory. MTD at 12. New York and California laws are not as restrictive. Rather, actual injuries are sufficient. *See e.g., Walters*, 2017 WL 1398660, at *2 (applying California law, finding “actual damages” of time spent credit monitoring following a data breach sufficient to state a claim for negligence); *Experian*, 2016 WL 7973595, at *3 (same, applying New York law).

As discussed in Section III.A.2, Plaintiff's out-of-pocket money and time expended due to the fraudulent charges were necessary, and constitute injuries under Article III.⁹ Indeed, courts consistently recognize that expenditures of time and money to remedy or mitigate harm from a data breach are sufficient to state a claim for negligence. *See e.g., Walters*, 2017 WL 1398660, at *2 (holding that plaintiff "alleged actual damages" for a negligence claim based on "out-of-pocket expenses" and the "value of time" incurred to "remedy or mitigate" a data breach); *Yahoo!*, 2017 WL 3727318, at *22 (following *Walters*); *see also Experian*, 2016 WL 7973595, at *3 (finding that plaintiff adequately plead a negligence cause of action when alleging that the plaintiff "spent approximately 3 hours addressing issues arising from the Data Breach, including addressing the fraudulent activity and checking his accounts and credit report for fraud.")

Further, Defendants compare this case to *Caudle*, but *Caudle* is factually incongruous. MTD at 12 (citing *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 282 (S.D.N.Y. 2008)) (holding that the theft of a laptop containing personal data resulted in no "serious concern" of future misuse when there was no proof the thief (1) accessed the personal data, (2) was "motivated by a desire" or "had the capabilities" to do so, or (3) ever accessed or misused the data). Here, criminal hackers successfully breached Defendants' systems, leading to the theft of over five million payment cards (including Plaintiff's), with approximately 125,000 payment card records sold as of April 1, 2018. SAC at ¶¶ 2, 4-9, 79. Comparing the theft of a single laptop, with no proof of misuse, to the theft of millions of payment cards is nonsensical.

Defendants also contend that Plaintiff's negligence and negligence *per se* claims are barred under the economic loss doctrine. MTD at 13. First and foremost, New York does not apply the

⁹ As discussed *infra*, Plaintiff also suffered benefit-of-the-bargain injuries, deprivation of value of her Customer Data, and an increased risk of future harm as a result of the Data Breach. *See* Section IV.A.1. Defendants make no argument that this injury is insufficient for the purposes of Plaintiff's negligence claim.

economic loss doctrine outside of products liability actions. *Sackin*, 278 F. Supp. 3d at 749 (denying defendant’s attempt to dismiss negligence claim in a data breach action, holding that the “economic loss rule . . . is inapplicable because the Complaint does not allege a products liability claim.”); *532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc.*, 96 N.Y.2d 280, 288 (2001) (same). Even if the doctrine did apply, New York recognizes exceptions to the economic loss doctrine where an independent duty exists under law *or* the defendant created a duty to protect the plaintiff’s customer data. *Sackin*, 278 F. Supp. 3d at 749-750 (holding that if a complaint “alleges breach of [independent] common law and statutory duties distinct from Defendant’s contractual duties[,]” the economic loss rule does not apply); *see also Experian Data Breach Litig.*, 2016 WL 7973595, at *3 (rejecting the application of the “economic loss rule” in a data breach class action when the plaintiff alleged that the defendant created duties to protect the data). Plaintiff alleged the same here. *See* SAC ¶¶ 67-74, 156-62, 186 (alleging that Defendants had a duty to maintain reasonable data security measures under Section 5 of the FTC Act); *id.* at ¶¶ 65, 125-26 (alleging that Defendants “undertook and owed a duty” to protect the Customer Data, and that Defendants further explicitly warranted to reasonably safeguard this data).

Defendants contend that the economic loss doctrine’s “special relationship” exception under New York¹⁰ and California law do not apply here, but fail to point to any authorities in the context of a data breach. MTD at 13. Under California law, courts have consistently recognized special relationships where, as here, plaintiffs provided their data to a business for a transaction or

¹⁰ Although Plaintiff maintains that, under New York law, the economic loss doctrine does not apply outside the scope of products liability cases, even if the doctrine did apply, the parties fall within New York’s “special relationship” exception. *Those Certain Interested Underwriters, at Lloyd’s, London, subscribing to Policy No. Z101663/003 v. Farley Grp.*, No. 1:12-CV-0707 GTS/FRT, 2015 WL 5602924, at *33 (N.D.N.Y. Sept. 23, 2015) (“Courts have found a special relationship and duty, for example, where defendants sought to induce plaintiffs into a business transaction by making certain statements or providing specific information with the intent that plaintiffs rely on those statements or information.” *Century Pac., Inc. v. Hilton Hotels Corp.*, No. 03 CIV. 8258 (SAS), 2004 WL 868211, at *8 (S.D.N.Y. Apr. 21, 2004) (same); *see* SAC ¶ 65 (alleging that Defendants’ website warrants to consumers that it would safeguard Customer Data).

agreement, the injuries from theft were foreseeable, and hackers stole the data. *See, e.g., Yahoo!*, 313 F. Supp. 3d at 1132 (finding a special relationship when plaintiffs alleged an “understanding that Defendants would adequately protect” their data, the injury from hackers was foreseeable and occurred, and defendants knew their data security measures were inadequate); *see also Corona v. Sony Pictures Entm’t, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *5 (C.D. Cal. June 15, 2015) (same, particularly when defendant experienced previous data breaches and did not expend adequate money to upgrade their security systems).

Plaintiff has pleaded substantially similar allegations. *See* SAC ¶¶ 22, 65, 118-119, 133 (alleging that Defendants promised on their website to safeguard Customer Data, and that to purchase Defendants’ items, Plaintiff provided her Customer Data, believing Defendants would safeguard it); *id.* at ¶¶ 9, 45, 132, 134 (alleging that inadequate data security measures would lead to a foreseeable risk of harm, particularly when Defendants experienced a previous data breach); *id.* at ¶ 23 (alleging that Plaintiff suffered fraudulent activity on her payment card associated with the breach); *id.* at ¶ 40 (alleging that Defendants failed to spend money to adequately maintain their data security features). In any event, the “determination of whether a special relationship exists is essentially a factual inquiry.” *Suez Equity Investors, L.P. v. Toronto-Dominion Bank*, 250 F.3d 87, 104 (2d Cir. 2001).¹¹

2. Plaintiff Has Adequately Alleged A Claim For Negligence *Per Se*

Next, Defendants proffer that Plaintiff’s negligence *per se* claim fails because she did not “adequately plead the requisite element of injury or damages.” MTD at 14. For the same reasons Plaintiff has adequately pleaded injuries for her negligence claim, Plaintiff has adequately pleaded injury for her negligence *per se* claim. *See* Section IV.B.1. Defendants further contend that, “[i]n

¹¹ For the same reasons discussed herein, Defendants’ argument that the economic loss doctrine bars Plaintiff’s negligence *per se* claim fails as well. MTD at 13 n.5.

the event that California law applies,” negligence *per se* is not recognized as an independent cause of action under California law. MTD at 14. To the extent the Court applies California law, Plaintiff respectfully requests this Court construe Plaintiff’s negligence *per se* claim as a traditional negligence claim, but apply the negligence *per se* doctrine. *Dent v. Nat’l Football League*, 902 F.3d 1109, 1117 (9th Cir. 2018) (“[W]e construe the [plaintiffs’] claim as a traditional negligence claim, but apply the negligence *per se* doctrine.”).

3. Plaintiff Has Adequately Pleaded Her Implied Contract Claim

Under California and New York law, an implied contract requires offer, acceptance, consideration, legal capacity, and may result from the party’s conduct. *Leibowitz v. Cornell Univ.*, 584 F.3d 487, 506–07 (2d Cir. 2009); *see also Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *8 (N.D. Cal. Sept. 14, 2016) (same).

California and New York courts have repeatedly recognized the existence of implied contracts when a company receives and maintains sensitive information in a transaction or agreement. *See, e.g., Sackin*, 278 F. Supp. 3d at 750 (holding that defendant “evinced an implicit promise” to safeguard plaintiffs’ data, particularly when the defendant’s “privacy policies” warranted as such); *Hameed-Bolden et al. v. Forever 21 Retail, Inc.*, No. CV18-03019 SJO (JPRX-x), 2018 WL 6802818, at *3 (C.D. Cal. Oct. 1, 2018) (finding an implied contract to safeguard consumers’ data in a retail data breach class action when plaintiffs alleged that defendants invited customers to “make purchases using their credit or debit cards”); *Castillo*, 2016 WL 9280242, at *9 (finding an implied contract to safeguard personal data in a data breach class action even though the defendant “made no explicit promises” to protect the data).

Here, Saks’ conduct, including explicit promises by Defendants to safeguard their customers’ data, gave rise to the implied contract. *See* SAC ¶ 65 (alleging that Defendants’

warranted to consumers on their privacy policy that “Protecting the security of your information is very important to us . . . [o]nce we receive your transmission, we will take reasonable precautions to secure and protect the information on our systems”);¹² *id.* at ¶¶ 118-20 (alleging that Plaintiff and class members provided their Customer Data to Defendants believing that Defendants would adequately safeguard the data).

Next, Defendants contend that the implied contract fails for lack of consideration because “[d]oing what one is already bound to do cannot be consideration.” MTD at 15. However, Defendants’ explicit promise in their privacy policy to safeguard the Customer Data is a voluntary promise, independent from any legal obligation. *Walters*, 2017 WL 1398660, at *2 (holding that a hotel-defendant’s statement in their privacy policy that they are “committed” to safeguarding customer privacy and personal information plausibly created an “an enforceable promise” which “is a voluntary duty not imposed by law and constitutes valid consideration.”)

Finally, Defendants contend that Plaintiff’s implied contract claim should be dismissed because she failed to show cognizable, actual damages. MTD at 16. However, as demonstrated *supra*, Plaintiff’s time and money expended as a result of the data breach classifies as actual damages. *See* Section III.A.2; *see also Hameed-Bolden*, 2018 WL 6802818, at *4 (holding that “actual and appreciable damages including out-of-pocket expenses as a result of the Data Breach” were sufficient injuries for an implied contract claim in a data breach class action). In any event, Defendants’ argument is premature as “[t]he existence of an implied contract is an issue of fact.”

¹² Because Defendants made this warranty, their contention that Plaintiff “alleges no facts giving rise to the inference that Defendants tacitly agreed” to protect Plaintiff’s data is belied by the plain words of the complaint. MTD at 16. Regardless, even without this promise, “[w]hen the customer uses a credit card for a commercial transaction . . . [t]here is an implicit agreement to safeguard the customer’s information to effectuate the contract.” *Irwin v. Jimmy John’s Franchise, LLC*, 175 F. Supp. 3d 1064, 1070 (C.D. Ill. 2016); *see also Castillo*, 2016 WL 9280242, at *9 (explaining that “[w]hile Seagate made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of [sensitive data] would not imply the recipient’s assent to protect the information sufficiently.”)

Castillo, 2016 WL 9280242, at *8. For these reasons, Plaintiff has adequately pleaded her breach of implied contract claim.

4. Plaintiff Has Adequately Alleged Her Unjust Enrichment Claim

A plaintiff sufficiently states a claim for unjust enrichment when alleging that the defendant was unjustly enriched at the plaintiff's expense, and that the defendant should be required to return its ill-gotten gains. *See Golden Pac. Bancorp v. F.D.I.C.*, 273 F.3d 509, 519 (2d Cir. 2001); *ChromaDex, Inc. v. Elysium Health, Inc.*, No. SACV 16-02277-CJC (DFMx), 2017 WL 7080237, at *4 (C.D. Cal. Nov. 28, 2017). Here, Plaintiff alleged that she “conferred a monetary benefit” and provided her Customer Data to Defendants when purchasing their goods and services, and in return, Defendants should have implemented adequate data security measures to protect this data, particularly when they made “substantial investments” to their stores in lieu of data security upgrades. SAC ¶¶ 40, 171-73. Plaintiff additionally alleges that she would not have made purchases at Defendants' stores had she known that Defendants failed to properly secure her Customer Data. *Id.* at ¶ 175.

Courts routinely recognize that such allegations sufficiently establish an unjust enrichment claim in the context of data breach class actions. *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 984 (N.D. Cal. 2016) (“*Anthem I*”) (sustaining plaintiffs' unjust enrichment claim in a data breach class action when plaintiffs alleged that defendants “should not be permitted to retain the [customers'] money” when it failed to “adequately implement” the “data security” practices plaintiffs paid for); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) (same, when the plaintiff alleged that she “would not have shopped” at defendant's stores had she known the defendant had inadequate data security practices); *Sackin*,

Inc., 278 F. Supp. 3d at 751 (same, when the plaintiffs alleged that the defendant retained the plaintiffs' monetary benefit, but chose not to spend money to sufficiently upgrade its data security).

Defendants proffer two arguments against Plaintiff's unjust enrichment claim. First, Defendants argue that Plaintiff "does not allege that she did not receive what she paid for" at Defendants' stores. MTD at 16-17. Defendants' arguments are belied by the plain words of the complaint. SAC ¶ 171 (alleging that Plaintiff "should have been entitled to have Defendants protect their Customer Data with adequate data security.") Plaintiff not only expected the goods she purchased, but also that her Customer Data would be reasonably safeguarded. As held in *Anthem I*, *Target*, and *Sackin*, this expectation is sufficient to establish an unjust enrichment claim.

Second, Defendants argue that "because Plaintiff's claim for unjust enrichment is based on the same core allegations as her claim for breach of implied contract, both California and New York [law] require its dismissal." MTD at 17-18. This argument ignores the plain language of Rule 8, permitting plaintiffs to plead alternative or duplicative theories. *See Astiana v. Hain Celestial Grp.*, 783 F.3d 753, 762 (9th Cir. 2015) (explaining that "cause[s] of action" which are "duplicative of or superfluous to [plaintiff]'s other claims" is "not grounds for dismissal") (citing to Fed. R. Civ. P. 8(d)(2)). Further, as many courts have recognized, when a defendant disputes the validity of the plaintiff's contract claim, the unjust enrichment claim should still proceed. *See, e.g., Sackin*, 278 F. Supp. 3d at 751-52 (denying defendant's argument that the plaintiffs' implied contract claim precludes their unjust enrichment claim when "Defendant's opposition suggests that it will dispute that Defendant agreed to be bound in an implied contract with Plaintiffs."); *see also Fero*, 236 F. Supp. 3d at 769-70 (same); *Anthem II*, 2016 WL 3029783, at *28 (same). Defendants explicitly dispute Plaintiff's implied contract claim. *See* MTD at 15-16. For these reasons, Plaintiff adequately pleaded her unjust enrichment claim.

C. Plaintiff's Statutory Claims Should Also Survive

1. Plaintiff Can Establish A Private Right of Action Under the Mississippi Consumer Protection Act¹³

Defendants argue that Plaintiff cannot bring a claim under the Mississippi Consumer Protection Act (“MCPA”) because the MCPA prohibits representative actions. MTD at 19. As an initial matter, Defendants’ argument is premature as it is outside the scope of a 12(b)(6) motion: whether Plaintiff has sufficiently pleaded her claim. *See Forth v. Walgreen Co.*, No. 17-CV-2246, 2018 WL 1235015, at *11 (N.D. Ill. Mar. 9, 2018) (holding that defendants’ argument that various consumer protection statutes “prohibit class actions” is “premature” because the question on a 12(b)(6) motion – “[w]hether Plaintiff ... can bring an individual claim” under the statutes – “is unaffected by whether the statute prohibits class actions”); *Sheet Metal Workers Local No. 20 Welfare & Benefit Fund v. CVS Health Corp.*, 221 F. Supp. 3d 227, 237 (D.R.I. 2016) (deferring question on whether consumer protection statutes’ bar on class actions applied to plaintiff’s claims to “the class certification stage.”)

Regardless, even if the Court was to decide this issue at this stage, Defendants’ position is inconsistent with the Supreme Court’s decision in *Shady Grove*, where the Supreme Court held that Federal Rule of Civil Procedure 23 “unambiguously authorizes any plaintiff, in any federal civil proceeding, to maintain a class action if the Rule’s prerequisites are met.” *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 406 (2010).¹⁴

¹³ Defendants’ header for its section suggests that Plaintiff “cannot establish a private right of action,” but Defendants solely discuss the MCPA’s purported bar on class actions and pre-suit requirements. MTD at 19. In fact, Defendants admit that the MCPA “creates private rights of action.” *Id.* For this reason, Plaintiff will assume Defendants concede that the MCPA allows for a private right of action.

¹⁴ Indeed, following *Shady Grove*, courts across the nation have recognized that where a state law categorically bars representative actions, it is trumped by Rule 23 in federal court. *See, e.g., Lisk v. Lumber One Wood Preserving, LLC*, 792 F.3d 1331, 1336 (11th Cir. 2015) (holding that Rule 23 trumps any statute with a class action bar “when all the statute does is prescribe who can bring a class claim based on the very same substantive conduct.”); *Suchanek v. Sturm Foods, Inc.*, 311 F.R.D. 239, 263–64 (S.D. Ill. 2015) (holding that Rule 23 trumps the categorical class action limitation found in Alabama, Tennessee, and South Carolina’s consumer protection statutes); 7A Charles Alan Wright,

Defendants further contend that Plaintiff's MCPA claim should be dismissed because she did not allege that she attempted to engage in the pre-suit dispute resolution process set forth under the MCPA. MTD at 20. However, Defendants' contention would require Plaintiff to plead her claim in a heightened fashion, which conflicts with Rule 8's notice pleading standard. *See, e.g., Braddock v. Orlando Reg'l Health Care Sys., Inc.*, 881 F. Supp. 580, 583–84 (M.D. Fla. 1995) (holding that Federal Rules of Civil Procedure displaces two of Florida's "specialized [pleading] hurdles for filing particular causes of action" because they run contrary to Rule 8); *Robinson v. Corr. Med. Assocs., Inc.*, No. 1:09-CV-01509-JOF, 2010 WL 2499994, at *4 (N.D. Ga. June 15, 2010) ("[T]he court finds that the affidavit requirement of [state statute] is contrary to the Federal Rules of Civil Procedure and does not apply in this case.") Therefore, Plaintiff had adequately pleaded a claim under the MCPA.

2. Plaintiff Has Alleged a Cognizable Injury Under The California Customer Records Act

As Defendants admit, an Article III injury is sufficient for standing under the California Customer Records Act ("CRA"). MTD at 20 (citing *Adobe*, 66 F. Supp. 3d at 1218) (holding that a plaintiff "establish[es] statutory injury under the CRA" when he alleges an "injury that satisfies Article III's injury-in-fact standard[.]"). As previously explained, Plaintiff suffered multiple injuries sufficient to confer Article III standing. *See* Section III.A. Further, Defendants' authority, *Adobe*, supports Plaintiff's position. *See Adobe*, 66 F. Supp. 3d at 1216-17 n.8 (holding that an "increased risk of harm" and "costs incurred to mitigate" harm from a data breach are sufficient damages under the CRA). For this reason, Defendants' contention that Plaintiff has not suffered a sufficient injury-in-fact to warrant Article III standing for her claims under §§ 1798.81.5 or 1798.82 of the CRA falls flat. MTD at 20.

et al., *Federal Practice & Procedure* § 1758 (3d ed. 2018) ("It now is clear that Rule 23 controls whether a class action may be maintained, regardless of a conflicting state law.")

Defendants remaining two arguments only challenge Plaintiff's claim under § 1798.82 of the CRA. MTD at 21. Specifically, Defendants contend that they provided sufficient notice to consumers because they provided substitute notice of the breach, which is permissible under the CRA. *Id.* Plaintiff does not dispute that the CRA allows for substitute notice. Rather, Plaintiff maintains that the *content* of Defendants' notice under the CRA was insufficient because the notice disclosure requires businesses suffering a data breach to provide specific information to California residents *regardless* of the notice's format. SAC ¶ 153 (explaining that, under Cal. Civ. Code §1798.82(d)(1), disclosures must be provided to consumers with specific headings and language). As Plaintiff alleges, Defendants' disclosure failed to provide the content in this format "to California Residents as required under Cal. Civ. Code Section 1798.82(d)(1)[.]" *Id.* at ¶ 154. Defendants' contention that Plaintiff never alleged that their "notice is insufficient" is belied by the SAC. MTD at 21. Defendants provide no argument or authority demonstrating that the content of their notice met the requirements of §1798.82(d)(1). *Id.*

Lastly, Defendants argue that Plaintiff cannot bring a claim under § 1798.82 because she cannot allege any injury stemming from Defendants' failure to provide adequate notice of its data breach. MTD at 21-22. However, no economic injury is required to state a claim under § 1798.82,¹⁵ as Defendants' violation of the CRA serves as an independent ground for Plaintiff to pursue injunctive relief under § 1798.84(e) of the CRA. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (holding that plaintiff need not allege a lack of injury based on the defendant's violation of the CRA to "pursue their injunctive relief claims under § 1798.84(e), which affords relief when a business violates, proposes to violate, or has violated" the CRA) (internal quotation marks omitted).

¹⁵ Plaintiff maintains that she adequately plead injuries for her cause of action under § 1798.81.5 for the reasons set forth above.

3. Plaintiff Has Alleged a Cognizable Injury Under The UCL

Next, Defendants argue that Plaintiff has not suffered an economic injury under the UCL. MTD at 22-23. As the California Supreme Court recognizes, “[t]here are innumerable ways in which economic injury [under the UCL] may be shown[,]” including, *inter alia*, “surrender[ing] in a transaction more, or acquire in a transaction less, than he or she otherwise would have . . . or [] be[ing] required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.” *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 323 (2011).

As discussed above, Plaintiff has alleged multiple economic injuries arising from the data breach, including out-of-pocket expenses in the form of time and money expended as a result of the Data Breach. SAC ¶ 22; *see* Section III.A. Indeed, an overwhelming number of courts recognize that out-of-pocket expenses and time spent in connection with a data breach are economic damages under the UCL. *See, e.g., Hameed-Bolden*, 2018 WL 6802818, at *4 (finding that plaintiffs adequately pleaded UCL injury when alleging that they “lost money and time” as a result of a data breach, including those “result[ing] of unauthorized charges on their debit and credit cards”).¹⁶

Plaintiff has also alleged benefit-of-the-bargain injuries suffered from purchasing items she otherwise would not have, had she known of Defendants’ inadequate data security, particularly when Defendants warranted her information would be safe. *Id.* at ¶¶ 23, 25, 65, 199. Courts applying the UCL in the context of data breach class actions have consistently recognized benefit-of-the-bargain damages as economic injuries. *See, e.g., Adobe*, 66 F. Supp. 3d at 1224 (approving

¹⁶ *See also Gordon*, 2018 WL 4620342, at *17 (holding that “time and effort spent addressing fraud” on financial accounts constitutes an “economic” injury); *Walters*, 2017 WL 1398660, at *2 (holding that the plaintiff “sufficiently alleged ‘actual damages’ under the UCL based on his ‘value of time’ incurred as a result of a data breach”); *Dieffenbach*, 887 F.3d at 829 (explaining that “[California] state courts have said that significant time and paperwork costs incurred to rectify [data breach] violations also can qualify as economic losses.”)

benefit of the bargain damages as an economic injury under the UCL when plaintiffs allege that they would spent less money on the defendant's products "had they known [defendant] was not providing the reasonable security [it] represented it was providing," explaining that it is "plausible that a company's reasonable security practices reduce the risk of theft of customer's personal data and thus that a company's security practices have economic value."); *Anthem II*, 2016 WL 3029783, at *43 (same, following *Adobe*); *Yahoo!*, 2017 WL 3727318, at *21 (holding that plaintiff has "adequately alleged standing under the UCL" under a "benefit of the bargain" theory when the plaintiff alleged that he would not have paid for the defendants' services had he known that the defendants' data security measures were inadequate).

Defendants proffer that Plaintiff's benefit-of-the-bargain injuries do not fall within the UCL because she did not allege that a portion of the purchased product's value was earmarked for data security. MTD at 23 (citing *Engl*, 2016 WL 8578096, at *9) (dismissing benefit-of-the-bargain damages when plaintiff did not allege a portion of products' value was "earmarked" for data security); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954 (D. Nev. 2015) (same). However, neither *Engl* nor *Zappos* considered this theory under the purview of the UCL. Indeed, the "earmark" argument advanced by Defendants' authorities has been explicitly rejected by courts considering the argument under the UCL. *Anthem II*, 2016 WL 3029783, at *13 (rejecting defendants' argument that the plaintiffs' "benefit of the bargain theory... fails because they do not allege facts showing that any alleged payments were earmarked for data security," explaining that "California courts have consistently rejected" this argument) (citing cases). For these reasons, Plaintiff has sufficiently alleged economic injury under the UCL.

D. Plaintiff's Declaratory and Injunctive Relief Claim Should Survive

Finally, Defendants argue that Plaintiff's injunctive relief and declaratory judgment claim fails because it cannot serve as an independent cause of action. MTD at 24. However, it is well-established that a plaintiff may seek declaratory relief under the Declaratory Judgment Act, and use it as a basis for injunctive relief. SAC §§ 180, 187 (seeking declaratory relief under the Declaratory Judgment Act and requesting various injunctive relief). *See In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) (denying, in a data breach class action, the defendant's argument that a plaintiff cannot maintain a standalone claim for "Injunctive and Declaratory Relief," holding that "[s]uch a claim is permissible under the Declaratory Judgment Act").¹⁷

IV. CONCLUSION

For these reasons, Plaintiff respectfully requests this Court deny the MTD in its entirety.¹⁸

Dated: January 25, 2019

FARUQI & FARUQI, LLP

By: /s/ Timothy J. Peter
 Timothy J. Peter
 tpeter@faruqilaw.com
 1617 JFK Blvd., Ste. 1550
 Philadelphia, PA 19103
 Tel: (215) 277-5770
 Fax: (215) 277-5771

Attorneys for Plaintiff Alexandria Rudolph

¹⁷ *See also Powell v. McCormack*, 395 U.S. 486, 499 (1969)) (holding that "[a] declaratory judgment can then be used as a predicate to further relief, including an injunction."); *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-at, 2018 WL 2128441, at *15 (N.D. Ga. Mar. 5, 2018) (allowing standalone declaratory judgment claim under the Declaratory Judgment Act to survive in a data breach class action); *First Choice Fed. Credit Union v. Wendy's Co.*, No. CV 16-506, 2017 WL 9487086, at *5 (W.D. Pa. Feb. 13, 2017) (same).

¹⁸ Plaintiff fully stands on her arguments submitted herein. However, to the extent the Court finds that any of Plaintiff's claims can be cured by amendment, Plaintiff respectfully requests leave to amend.